Security Architecture Work Group

Monday June 11, 2001
1:30 p.m. to 3:00 p.m.
Executive Building Video Conference Room
521 South 14th Street,
Lincoln, Nebraska

Minutes

A. Participants

Allan	Albers	HHSS/IS&T
Rod	Armstrong	Nebrask@ Interactive
Mahendra	Bansal	DNR
Jason	Everett	ESU 10
Jerry	Hielen	IMServices
Sandy	LaLonde	IMServices
George	McMullin	Nebraska CERT / USSTRATCOM
Jon	Ogden	Roads
Leona	Roach	University of Nebraska Computing Services Network
Steve	Schafer	Nebraska CIO

1) Security Procedures Documentation

Jerry Hielen and Sandy LeLonde reviewed progress on the draft documents. They invited discussion regarding scope and deliverables. They had received some comments on earlier drafts, which they have tried to incorporate. The templates constitute a complete awareness program. There will be a handbook for the general employee. This will be a comprehensive set of rules, rather than general policies or procedures. The one exception will be procedures for reporting a security incident. Another handbook is targeted to computer services employees. It will be made up of both procedures and specific rules. The purpose is to help the IT employee incorporate security matters into the employee's responsibilities. The third handbook is for the security officer. It will include procedures and tutorials on how to carryout security activities, such as conducting a risk assessment, assembling a security team and preparing a business impact analysis. It will include checklists for the security officer.

The electronic templates offer opportunities for sophistication in the future, such as masking certain sections, if they are not needed. For now, the templates will be developed for posting in electronic form, but they will not incorporate these features.

One source of confusion is the use of terminology. The terms policy, standards, procedures, and rules are often used interchangeably. How we use each term is not as important as the need for consistency. After a short discussion, there was general consensus on the following definitions:

- Policy: Statements of goals and principles adopted by the NITC;
- Standards: Activities that can be observed or measured to determine whether they are being carried out; these may apply to either individuals or organizations.
- Rules: Specific guidelines governing behavior and actions of individuals;
- Procedures: Guidance for how to implement specific standards or rules.

- Organization: A generic term that encompasses state agencies, political subdivisions, educational institutions or other entities.
- Systems: Includes computer hardware, operating systems, applications, and networks.

The prototypes of the templates were finished as scheduled by May 30. The first draft of the templates will be ready by June 19. Jerry Hielen will test the usability of the templates by using the procedures to develop a security program for IMServices.

Discussion identified several areas of concern. How to keep the templates up to date will be an on-going problem. Although frequent and widespread changes are not likely, someone will need to review the templates periodically to be sure they are still current. Widespread adoption of the templates with limited modification by organizations will make maintenance easier. Who is responsible for maintaining the templates is also a concern. Identifying a custodian and establishing a process for reviewing and changing the templates will be important to their long-term success.

There was also discussion about implementation. In particular, some participants asked how the policies and procedures would be enforced. They argued that some enforcement mechanism would be needed for the eventual success of any security program, especially for issues that cut across organizational boundaries. Participants pointed out several existing enforcement mechanisms that might be used to encourage compliance with security policies and procedures. These include the Internal Revenue Service and HIPAA compliance requirements at the federal level. State level options include financial audits, special security audits, self-assessments, peer review teams, and general information sharing.

The NITC adopted planning and project management guidelines that require biennial agency comprehensive technology plans. These plans could incorporate a security self-assessment.

2) Other Implementation Options

a. Business Case Outline – Steve Schafer reported he has not made much progress to date on drafting a business case for policy makers. He invited suggestions for content. Developing the business case is an iterative process involving policies and procedures, planning, and assessments of exposure to potential problems.

b. CERT Conference – The CERT Conference is August 6 to 10. Steve Schafer will make a presentation on the state's security policies and procedures on Wednesday afternoon, August 8 (3:30).

c. Fall Security Technical Forum (early November?) – No discussion.

3) Next Meeting Date

The next meeting is Monday July 9 at 1:30, same locations.